ABSTRACT

Requests issuing on a host computer are intercepted and stalled prior to sending to target computer systems. The requests are analyzed to determine whether they are suspicious. Requests determined to be suspicious are added as request entries to a request database. Each time a request entry is added to the request database, a determination is made whether malicious code activity is detected on the host computer system. Upon a determination that malicious code activity is detected, a notification of the malicious code detection is generated and protective actions are implemented, such as terminating the request. Requests not determined to be suspicious or to indicate malicious code activity are released for sending to the target computer systems.